クラウドネットワークにおける情報セキュリティの飛躍的強化のための格子暗号の実用性に関する調査研究

代表研究者　　深　瀬　道　晴　　早稲田大学グローバルエデュケーションセンター非常勤講師・秀明大学英語情報マネジメント学部非常勤講師

1 はじめに

クラウドコンピューティング社会を本格的に実現させる上で、情報セキュリティが大きな阻害要因となっている。利便性とセキュリティの相反する要求に直面するクラウドネットワークの普及には、利便性を保ったままセキュリティを強化する要素技術の開発が不可欠である。クラウドネットワーク上において機密データの暗号化は必須である。しかし、機密データに処理を施すためにはクラウドネットワーク上で復号する必要があり、このとき情報セキュリティリスクが高まってしまう。この問題を解決するために、暗号化データを復号することなく直接暗号化データに任意の処理を施すことで、元のデータの操作を可能にする完全準同型性が重視されている。本調査研究において、完全準同型性を有する格子暗号(Lattice-Based Cryptography)の実用化に向けて重要な評価基準となる安全性を分析する。格子暗号の安全性と密接に関連する格子の最短ベクトル問題(The Shortest Vector Problem, SVP)に関して、以下の 3 つの研究課題を実施する。

1. 格子の最短ベクトルを効率的に求めるために設定した探索空間に関して、探索空間に含まれる格子ベクトルのノルムの分布が正規分布を近似することを実験的に示す。探索空間に含まれる格子ベクトルのノルムの分布が正規分布を近似することは既に理論的に示されており、最短ベクトルが求まる確率を導出することができる。理論的に導出された確率の正当性を、当該実験によって裏付けする。また、探索空間の設定法の有効性に根拠を与える最短ベクトルの特徴に関する理論を、実験によって検証する。
2. 最短ベクトル探索に用いる格子基底の質が探索効率に及ぼす効果について分析する。格子基底の質を測る指標としては、基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの和を用いる。探索効率を測る指標としては、探索空間の大きさと探索空間における最短ベクトルの包含確率を用いる。最短ベクトルが分かっている格子について、その格子基底のグラム・シュミット直交ベクトル列の二乗ノルムの和と、探索空間が最短ベクトルを含む確率を求めることで、それらの関係を実験的に明らかにする。
3. 最短ベクトル探索に用いる探索空間を設定する上で、短いベクトルを効率的に求めるためには、探索空間の大きさを決定するパラメータを適切に設定しなければならない。適切なパラメータを理論的に導出することは難しく、実験的に効果を検証したパラメータを用いる必要があり、パラメータの設定には困難が伴う。そこで、この困難を解消するために、探索空間に関するパラメータを精緻に設定することなく、適切な探索空間を構成するために遺伝的アルゴリズム (GA) を導入する。GA によって進化した探索空間が、短いベクトルを含み得るかを実験によって検証する。

2 SVP アルゴリズムの求解確率に関する統計分析

SVP アルゴリズムによる求解確率を理論的に導出することは、格子暗号の安全性を検証する上で重要である。ここでは、改良型 SVP アルゴリズムについて、理論的に提示された求解確率の正当性を実験的に裏付ける。求解確率の導出は、探索空間に含まれる格子ベクトルのノルムの分布が正規分布を近似するという仮定に基づいている。そこで、理論的に導出された求解確率の正当性を裏付けるために、探索空間に含まれる格子ベクトルのノルムの分布が正規分布を近似するという仮定を実験的に検証する。また、論文[12]において導入された格子ベクトルに対応する自然数表現に関して、探索空間の設定法の有効性に根拠を与える最短ベクトルの特徴に関する理論を、実験によって検証する。

2-1 改良型 SVP アルゴリズムの概要

格子暗号では、ベクトル空間に規則正しく配置された無数の点（格子）のうち、原点に最も近い点、すなわち、最短ベクトルが秘密鍵に関連する情報となる。したがって、格子暗号における解読は、格子の中から最短ベクトルを求めることに相当するため、より高次元で高速に求解可能な SVP アルゴリズムが格子暗号の安全性検証の重要なツールとなる。既存の SVP アルゴリズムとして、LLL アルゴリズム（[6]）、BKZ アルゴリズム（[10]）、また、RSR アルゴリズム（[11]）など多くのアルゴリズムが提案されている。これらの SVP アルゴリズムの性能評価を行うために、格子暗号解読の標準的なターゲットとして、SVP Challenge（[9]）が公開されている。SVP Challenge の解読競争においては、RSR アルゴリズムの改良型 SVP アルゴリズム（[2]、[12]）の柏原・照屋による実装プログラムが最も高次元において解読している。そこで、本研究では、改良型 SVP アルゴリズムを対象として実験を実施した。

2-2 最短ベクトル探索の成功と格子基底の質の関係

改良型 SVP アルゴリズムでは、格子を表現する基底に対応するグラム・シュミット直交ベクトル列の幾何的特徴に基づいて、探索空間を規定する。ここでの幾何的特徴とは、LLL アルゴリズムや BKZ アルゴリズムによって処理された基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムが減少幾何数列を近似することである。この特徴に基づいて規定した探索空間に含まれる格子ベクトルのノルムの分布は、中心極限定理により、正規分布を近似することが理論的に示されている。正規分布に関する理論に従うと、探索空間に含まれる格子ベクトルのノルムの期待値は、グラム・シュミット直交ベクトル列の二乗ノルムの和（GS 和）に比例する。したがって、GS 和が小さい程、短い格子ベクトルが得られる。さらに、GS 和によって最短ベクトルの求解確率を算出することができる。以上から、GS 和がより小さい基底が、より質の高い基底と考えることができる。そのため、改良型 SVP アルゴリズムでは、基底の GS 和を下げながら、短い格子ベクトルの探索を行う。

改良型SVPアルゴリズムの性能に理論的根拠を与える正規分布の仮定を、実験的に検証した。図1において、SVP Challenge の解読競争において用いられる次元 120 の格子において規定した探索空間に含まれる格子ベクトルのノルムの分布を示す。図 1 には、実験的に求めた格子ベクトルのノルムの分布の他に、理論値に基づく正規分布の確率密度関数も示されている。図 1 から、探索空間に含まれる格子ベクトルのノルムは、正規分布を非常に高い精度で近似していることが分かる。また、実験的に求めた格子ベクトルのノルムの平均と分散はそれぞれ、2.7×10^{7}、1.049×10^{13} であった。一方、理論的に求めた平均と分散はそれぞれ、2.656×10^{7}、1.047×10^{13} であった。このことから、実験値が理論値を高い精度で近似していることが示された。

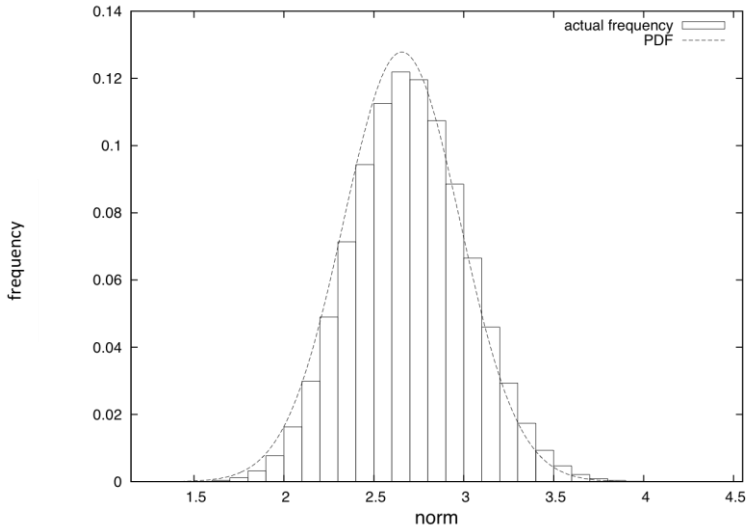

図１　探索空間に含まれる格子ベクトルのノルムの実際の分布と理論値に基づく正規分布の確率密度関数

また、改良型 SVP アルゴリズムの汎用性を検証するために、上記実験を、SVP Challenge の格子とは別のク

ラスの格子に対して行った。別のクラスの格子として、GGH 格子（[4]）、Micciancio's GGH 格子（[8]）、そして、NTRU 格子（[5]）を対象とした。GGH 格子及び Micciancio's GGH 格子は格子の特徴自体は非常に異なるが、SVP Challenge の格子と同様に、グラム・シュミット直交ベクトル列の幾何的特徴を満たすことが知られている。一方、NTRU 格子はグラム・シュミット直交ベクトル列の幾何的特徴を部分的にしか満たさないことが知られている（[7],[3]）。このように非常に異なる特徴を持つ３つのクラスの格子に対して、探索空間に含まれる格子ベクトルのノルムの実際の分布が理論値に基づく正規分布を近似するかを実験的に検証した。その結果、GGH 格子、Micciancio's GGH 格子、そして、NTRU 格子において、探索空間に含まれる格子ベクトルのノルムが正規分布を非常に高い精度で近似していることが検証された。この実験から、SVP Challenge の格子の他に、非常に異なる特徴を持つ３つのクラスの格子に対しても、改良型 SVP アルゴリズムを適用できることが示された。特に、グラム・シュミット直交ベクトル列の幾何的特徴を部分的にしか満たさない NTRU 格子に対しても、適用可能であることが示された。このことから、改良型 SVP アルゴリズムの汎用性、すなわち、別のクラスの格子に対する応用可能性が示された。

2-3 格子の自然数表現に関する最短ベクトルの特徴の分析

改良型 SVP アルゴリズムでは、格子の基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムが減少幾何数列を近似するという特徴に基づいて、探索空間を規定する。ここで、探索空間の規定の仕方は、最短ベクトルに対応する自然数表現が、0-1 からなる自然数列からなるという仮定に基づいている。そして、0-1 からなる自然数列において、1 が出現する頻度は非常に低く、出現する場所は自然数列の後半部分であり、例外的に 2 以上の自然数が出現することもあるがその頻度は非常に低いという仮定を置いている。この仮定は、論文[11]におけるグラム・シュミット直交ベクトル列の二乗ノルムに関する幾何的仮定から理論的に導くことができるが、ここでは、実験によって検証する。

実験では、SVP Challenge の解読競争において用いられる次元 120、126、128、130 の格子、及び、それぞれの格子における最短ベクトルを対象とした。それぞれの次元における最短ベクトルについて、対応する自然数表現における 1 以上の自然数が出現する頻度を計算した結果、全ての次元において、非常に低い頻度になることが示された。具体的に、自然数表現における全自然数の個数に対して、15%程度の頻度でしか 1 以上の自然数が出現しないことが示された。また、2-2 節の実験と同様に、GGH 格子、Micciancio's GGH 格子、そして、NTRU 格子においても、最短ベクトルに対応する自然数表現において、1 以上の自然数が出現する頻度を計算した結果、SVP Challenge の格子と同様に、非常に低い頻度になることが示された。

3 最短ベクトル探索に用いる格子基底の質が探索効率に及ぼす効果に関する分析

論文[2]においては、格子基底の GS 和が小さい程、探索空間に短い格子ベクトルが含まれる確率が大きくなることが示された。しかし、格子基底の GS 和の大小と短い格子ベクトルを得るために必要となる探索空間の大きさとの関係については分析されなかった。そこで、最短ベクトルの探索手法について、探索に用いる基底の GS 和が探索効率に及ぼす効果に関する実験を実施した。格子基底の質を測る指標として、基底に対応する GS 和を用いた。また、探索効率を測る指標として、探索空間の大きさと最短ベクトルを含む確率を用いた。最短ベクトルが分かっている格子について、その格子基底の GS 和と、探索空間が最短ベクトルを含む確率を求めることで、それらの関係を実験的に明らかにした。

本研究では、最短ベクトルが分かっている格子として、NTRU 格子を用いた。NTRU 格子に対して規定した探索空間における最短ベクトルの包含確率については、論文[3]において分析されている。論文[3]では短い格子ベクトルを得るのに適した探索空間の形が提案された。しかし、同一の形の探索空間を用いた場合でも基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの傾向の違いによって短い格子ベクトルが求まる頻度に大きな差が生じることが確認されたため、グラム・シュミット直交ベクトル列の二乗ノルムの傾向を示す GS 和の指標を論文[2]において導入した。本研究では、論文[2]において分析されなかった基底の GS 和の大小と短い格子ベクトルを得るために必要となる探索空間の大きさとの関係について実験をした。本研究における実験の結果、GS 和の異なる基底を用いて、基底の GS 和がより小さい程、探索空間に最短ベクトルが含まれる確率がより大きくなることが示された。

3-1 探索効率の分析

まず、短い格子ベクトルを得るために必要となる探索空間の大きさと GS 和の関係について検証した。以下に、実験の手順を示す。

[実験の手順]

1. 探索空間の大きさを変化させた場合において、探索で得られる格子ベクトルのノルムの変化の仕方を調べる。そのために、基底を固定して、探索空間の大きさを変化させ、探索で得られる格子ベクトルのノルムの最小値を計算する。
2. 探索空間を変化させる効果と GS 和の違いによる効果とを比較するために、上記と同様の計算を、GS 和の異なる別の基底に対して行う。

実験の結果、GS 和の小さい基底を用いることで、短い格子ベクトルを得るために必要となる探索空間の大きさを縮小できることが示された。例えば、GS 和が小さい基底では、GS 和が大きい基底よりも 1/1913 の大きさの探索空間において、より短い格子ベクトルが得られた。また、探索空間の大きさを決定するパラメータは２種類あるが、それぞれのパラメータ調整による効果、すなわち，探索空間に含まれる格子ベクトルのノルムの変化を検証した。その結果、一方のパラメータの設定次第では、探索空間を大きくしてもほとんど効果が得られないことが分かった。

3-2 最短ベクトルを含む確率の分析

3-1 の実験においては、最短ベクトルではなく、一定水準の短いベクトルについて実験を行った。ここでは、一定水準の短い格子ベクトルではなく、最短ベクトルについて実験を行う。NTRU 格子では、格子の次元 n について、最短ベクトルが n/2 個含まれている。例えば、格子の次元 n について、n=214 のとき、NTRU 格子には 107 個の最短ベクトルが含まれている。実験では、GS 和の異なる 45 個の基底について、探索空間が最短ベクトルを 107 個のうち何個含むかを計算する。ここで、探索空間が最短ベクトルを含む確率として、最短ベクトルが探索空間に含まれる頻度（探索空間に含まれる最短ベクトルの個数を探索空間の大きさで割った値）を計算する。

まず、探索空間が比較的小さい場合について、最短ベクトルが探索空間に含まれる頻度を計算した。ここでは、2369935 個の格子ベクトルを含む探索空間を用いた。このとき GS 和の異なる 45 個の基底について、最短ベクトルが探索空間に含まれる頻度を図 2 に示す。ここで、GS 和を説明変数、最短ベクトルが探索空間に含まれる頻度を非説明変数として、線形回帰をして、傾きが 0 であるという帰無仮説を検定した。統計ソフト R を用いた検定の結果、p 値が 0.003596 で 0.05 より小さいので、有意水準 5%において帰無仮説が棄却された。

次に、探索空間が比較的大きい場合について、最短ベクトルが探索空間に含まれる頻度を計算した。ここでは、93178047048 個の格子ベクトルを含む探索空間を用いた。このとき GS 和の異なる 45 個の基底について、最短ベクトルが探索空間に含まれる頻度を図 3 に示す。図 2 の場合と同様に、GS 和を説明変数、最短ベクトルが探索空間に含まれる頻度を非説明変数として、線形回帰をして、傾きが 0 であるという帰無仮説を検定した。統計ソフト R を用いた検定の結果、p 値が 0.00459 で 0.05 より小さいので、有意水準 5%において帰無仮説が棄却された。

以上の実験から、基底の GS 和は探索空間に最短ベクトルが含まれる頻度の要因として認められるという結論を得た。図 2 と図 3 の場合それぞれにおいて、線形回帰の結果、傾きの符号は負であり、このことから、基底の GS 和が小さい程、探索空間に最短ベクトルが含まれる頻度が大きくなると判断できる。したがって、最短ベクトルを探索する上では、基底の GS 和を可能な限り下げてから探索を行うべきであると考えられる。

3-3 基底の質を GS 和によって測ることについて

本研究の実験において、異なる基底に関する実験条件として、それぞれの基底の GS 和を用いた。ここで、基底の質として GS 和の指標を用いる意義について理解するために、異なる２つの基底 B と B'のそれぞれについて、基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムの対数値を、図４に示す。

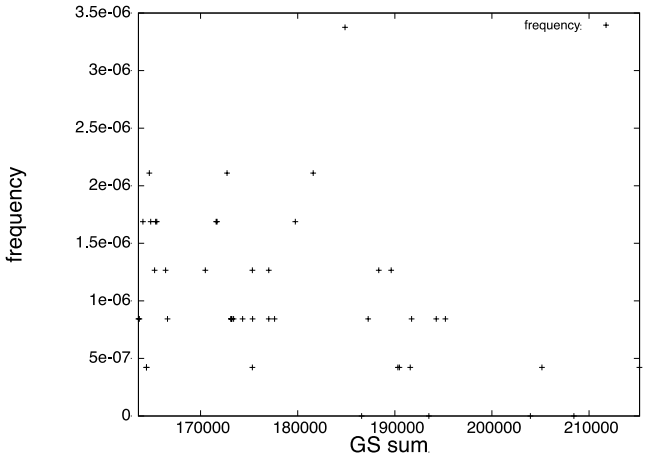

図２　探索空間が小さい場合における GS 和と最短ベクトルが探索空間に含まれる頻度の関係

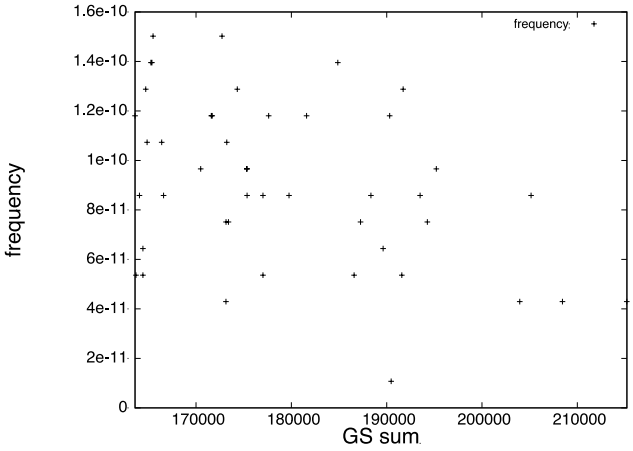

図３　探索空間が大きい場合における GS 和と最短ベクトルが探索空間に含まれる頻度の関係

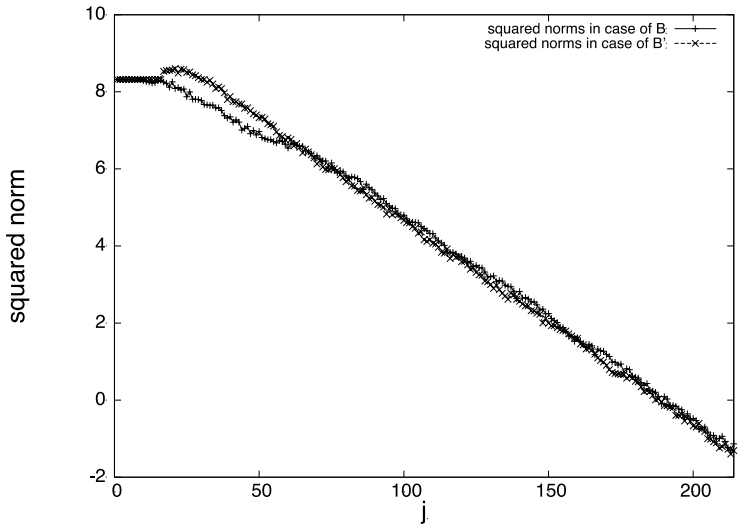

図４　異なる２つの基底のグラム・シュミット直交ベクトル列に関するベクトルのインデックスと二乗ノルムの関係

図４から、j=1 から j=20 辺りのインデックスにおいては二乗ノルムの値はほとんど等しいが、j=20 から j=50 辺りのインデックスにおいては、B の二乗ノルムの値の方が小さいことが分かる。一方で、j=50 以降の後半のインデックスにおいては、B'の二乗ノルムの値の方が小さい傾向が分かる。GS 和の指標を導入する利点は、個々の二乗ノルムの値の大小ではなく、上記で見たような全ての二乗ノルムの傾向を、1 つの数値で提示できることである。

4 SVP アルゴリズムのパラメータ設定における遺伝的アルゴリズムの適用

改良型 SVP アルゴリズムで用いる探索空間を設定する上で、短い格子ベクトルを高速に求めるためには、探索空間の大きさを決定するパラメータを適切に設定しなければならない。具体的に、短い格子ベクトルが求まる頻度を高く維持しながら、探索空間をより小さく設定する必要がある。しかし、このような適切なパラメータを理論的に導出することは難しく、実験的に効果を検証したパラメータを用いる必要があり、パラメータの設定は困難である。特に、3-1 節の実験において見たように、探索空間の大きさを決定するパラメータは２種類あり、設定の仕方が適切でないと探索空間の大きさに対して、ほとんど効果が得られない場合

もある。ここでは、最初に探索空間の２種類のパラメータを出鱈目に設定し、最初の探索空間を基点にして、適切な探索空間を構成するために遺伝的アルゴリズム（GA）を導入する。GA によって進化した探索空間が、短い格子ベクトルを含み得るかを実験によって検証する。

4-1 GA を導入したベクトル探索の流れ

改良型 SVP アルゴリズムで用いる適切な探索空間を GA によって構成し、短い格子ベクトルを求める手順を以下に示す。

[GA による探索]

1. 探索空間の大きさを決定する２種類のパラメータを出鱈目に設定し、最初の探索空間を規定する。
2. 最初の探索空間に含まれる格子ベクトルに対応する全ての自然数表現を、第一世代の個体とする。
3. 全ての個体に対して、成績評価を行う。個体の成績は個体に対応する格子ベクトルのノルムに応じて算出し、算出した成績により個体を選別する。
4. 成績評価の際に、最短ベクトルが求まれば、計算を終了する。
1. 選別された全ての個体に対して、一定の確率で交叉処理を施し、新しい個体群を生成する。
5. 新しい個体群に対して、一定の確率で突然変異処理を施す。
6. 全ての新しい個体群を次の世代とし、3 に戻る。

SVP アルゴリズムに対して GA を導入した研究として、Ding 等の研究（[1]）がある。Ding 等は GA における個体の表現に格子ベクトルの整数表現を変換したビット列を用いている。一方、本研究では、格子の整数表現ではなく、格子の自然数表現を用いる。また、本研究では、格子の自然数表現そのものを個体表現に用いる。

4-2 探索効率の分析

4-1 で示した GA による探索において、GA によって進化した探索空間が、短い格子ベクトルを含み得るかを実験によって検証した。以下に、実験の手順を示す。

[実験の手順]

1. 探索空間の大きさを決定する２種類のパラメータを出鱈目に設定し、最初の探索空間を規定し、GA による探索を行う。
2. 各世代において、全ての個体について、探索空間の設定に用いた基底に対応するグラム・シュミット直交ベクトル列の二乗ノルムを縮小し得るかを検証した。

実験の結果、最初の探索空間では、二乗ノルムを縮小する個体は存在しなかったが、後の世代では二乗ノルムを縮小する個体が発生する例が確認された。例えば、次元 111 の格子を用いた探索において、94 番目の世代において二乗ノルムを縮小する個体が発生した。

5 まとめと本調査研究に関する将来展望

本調査研究では、クラウドネットワークにおける情報セキュリティの強化を長期構想として、以下の 3 つの研究課題を実施した。

1. SVP アルゴリズムの求解確率に関する統計分析
2. 最短ベクトル探索に用いる格子基底の質が探索効率に及ぼす効果に関する分析
3. SVP アルゴリズムのパラメータ設定における遺伝的アルゴリズムの適用

研究課題 1 及び研究課題 2 において、改良型 SVP アルゴリズムの性能に根拠を与える統計的仮定と基底の幾何的性質に関する仮定を実験的に検証した。格子暗号の安全性検証のためには、SVP をより高次元で解くアルゴリズムを提示する必要がある。本研究課題では、格子暗号解読の標準的なターゲットである SVP Challenge において最も高次元での解読に用いられた改良型 SVP アルゴリズムに対して性能分析をした。また、研究課題 3 において、改良型 SVP アルゴリズムにおいて用いられる探索空間の効果的な構成法に関する

研究を実施した。ここでは、GA を適用して、出鱈目に設定したパラメータで構成された探索空間を、短いベクトルを含む探索空間に進化させることができることを示した。

格子暗号は、暗号化データを復号することなく直接暗号化データに任意の処理を施すことで、元のデータの操作を可能にする完全準同型暗号を実現することで知られていることに加えて、量子コンピュータを用いた効率的な解読アルゴリズムがまだ開発されていない、すなわち、量子コンピュータを用いても解読できないことが知られている。一方、標準的な公開鍵暗号として広く普及している RSA (Rivest Shamir Adleman) 暗号や楕円曲線暗号 (Elliptic Curve Cryptography, ECC)は、量子コンピュータによって効率的に解読されることが知られており、量子暗号実現後の脆弱化が指摘されている。そのため、格子暗号は、次世代暗号の重要な候補であり、格子暗号の安全性検証は情報セキュリティ分野における重要テーマである。本研究の将来展望は、SVP をより高次元で解くアルゴリズムを開発・改良すること、すなわち、格子暗号の安全性検証の確かなツールを構築することである。格子暗号の安全性検証のツールの構築は、格子暗号の実用化のために必須であり、クラウドネットワークにおける情報セキュリティの強化に寄与するものと考えられる。SVP アルゴリズムの開発・改良においては、探索の高効率化、すなわち、適切な探索空間の構成が必要である。適切な探索空間の構成のためには、適切なパラメータの設定と探索空間を構成するために用いる格子基底の質を向上させることが重要である。適切なパラメータの設定のためには、本調査研究で用いた遺伝的アルゴリズムを適用した手法を拡張・改良する。そして、格子基底の質を向上させるためには、SVP アルゴリズムの求解確率と格子基底の GS 和に関する分析を応用する。また，現在、本調査研究において考案した手法を探索に組み入れて実験を実施中である。実験結果については、SVP アルゴリズムの性能評価を行うための標準的なターゲットである SVP Challenge に順次登録していく予定である。

【参考文献】

[1] Ding, D., Zhu, G., and Wang, X.: A Genetic Algorithm for Searching Shortest Lattice Vector of SVP Challenge, Cryptology ePrint Archive, Report 2014/489, (2014).

[2] Fukase, M., Kashiwabara, K.: An Accelerated Algorithm for Solving SVP Based on Statistical Analysis, JIP, vol.23, no.1, pp. 67-80, (2015).

[3] Fukase, M., Yamaguchi, K.: Exhaustive Search for Finding a Very Short Vector in High-Dimensional Lattices. Proceedings (short papers) of IWSEC 2010, pp. 26-41, (2010).

[4] Goldreich, O., Goldwasser, S. and Halevi, S.: Public-Key Cryptosystems from Lattice Reduction Problems, CRYPTO 1997, vol. 1294 of LNCS, pp. 112–131, (1997).

[5] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. Proceedings of ANTS III, vol. 1423 of LNCS, Springer-Verlag, pp. 267-288, (1998).

[6] Lenstra, A.K., Lenstra, H.W., Lovasz, L.: Factoring Polynomials with Rational Coefficients. Mathematische Ann., vol. 261, pp. 513-534, (1982).

[7] Ludwig, C.: Practical Lattice Basis Sampling Reduction, PhD thesis, TU Darmstadt (2005).

[8] Micciancio, D.: Improving Lattice Based Cryptosystems Using the Hermite Normal Form, CaLC2001, vol. 2146 of LNCS, pp. 126–145, (2001).

[9] Schneider, M. and Gama, N.: SVP Challenge, available from ⟨http://www.latticechallenge.org/svp-challenge/⟩.

[10] Schnorr, C.P., Euchner, M.: Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. Math. Programming, vol. 66, pp. 181-199, (1994)

[11] Schnorr, C.P.: Lattice Reduction by Random Sampling and Birthday Methods. STACS 2003, vol. 2607 of LNCS, Springer-Verlag, pp. 145-156, (2003).

[12] 深瀬道晴,柏原賢二.:“格子の最短ベクトル問題における探索空間の特定”, 情報処理学会研究報告, Vol.2013-CSEC-62, pp.1-6 (2013)

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
An Accelerated Algorithm for Solving SVP Based on Statistical Analysis	Journal of Information Processing, Vol.23, No.1, pp.67-80	2015. 1
格子の最短ベクトル問題において格子基底の質が探索効率に及ぼす効果について	情報処理学会研究報告, Vol.2015-CSEC-70,No.5, pp.1-6	2015. 7
Technical University of Darmstadt 格子暗号解読コンテスト・次元 109 において求解	SVP Challenge: Hall of Fame,http://www.latticechallenge.org/svp-challenge/	2016. 3